Microelectronics Journal 67 (2017) 169–175

Contents lists available at ScienceDirect

Microelectronics Journal

journal homepage: www.elsevier.com/locate/mejo

A multi-port low-power current mode PUF using MOSFET current-division deviation in 65 nm technology

Gang Li, Pengjun Wang*, Yuejun Zhang, Huihong Zhang

Institute of Circuits and Systems, Ningbo University, Ningbo 315211, China

ARTICLE INFO

Keywords:
Physical unclonable function (PUF)
Multi-port
Low-power
Current mode
Current-division

ABSTRACT

Physical unclonable function (PUF) is a promising hardware security primitive for secure key generation and chip identification. This paper proposes a multi-port and low-power PUF based on MOSFET current-division deviation. Owing to the multi-port, it can parallelly generates multi-bit identifications (IDs) in one clock cycle. Moreover, with the MOSFET current-division array operating at sub-threshold region, it displays a low power consumption characteristic. As an embodiment, a 32-port PUF is implemented with full-custom design on 65 nm CMOS process, wherein the layout area and the power dissipation are 35178 μm^2 and 10.3 μW (@1.2 V/ 100 MHz), respectively. Post-layout simulation results show that it has a high performance in terms of randomness and uniqueness. In addition, it exhibits a worst case reliability of 98.62% over temperature range of –40 °C to 120 °C and 10% fluctuations in supply voltage, indicating an encouraging reliability and effectiveness.

1. Introduction

Over decades, counterfeit hardware has imposed a great demand of highly secure chip authentication technique. Fake parts are frequently seen in some security-sensitive industries, such as banking and national defense. To reduce the high risk of unauthentic chips, a number of advanced techniques have been developed [1]. Among numerous techniques, as a textural feature identification technology in the field of silicon substrate ICs, physical unclonable function (PUF) attracts special attentions due to its unique way for hardware security strengthen [2–4]. By capturing IC manufacturing process variations, PUF can produce a large number of identifications (IDs) which have features of unclonability, randomness, uniqueness, and reliability. Unclonability means that it is extremely difficult to counterfeit a PUF with the same challenge response pairs (CRPs) through physical method, although some PUFs are cloneable through mathematical ways [5,6]. Randomness refers to the random distribution of PUF IDs. Uniqueness is the ability to uniquely identify a PUF instance, which primarily depends on the sensitivity of deviation generating circuit to process variations. Reliability refers to the ability to produce the same IDs under varying environmental conditions, which usually need the help of error correction codes (ECCs) [7–9]. All these characteristics render PUF to have potential applications in the fields of information security, such as secure key generation [7,8], device authentication and IP protection [9–11].

Except for the advantages of PUF, power consumption still restricts the application of PUF [12]. Therefore, we are motivated to explore the feasibility of designing low-power PUF. In additions, the PUF should be able to generate multi-bit IDs within one clock cycle when used together with some specific cryptographic algorithms, such as DES, AES, and ECC. For instance, the cipher key for AES algorithm [13] is a sequence with 128,192 or 256 bits. To reduce power dissipation, a few PUF implementations have been reported recently [12,14–16]. However, they are single-port PUFs. If a multi-port PUF is formed by simply combining multiple single-port PUFs, both the chip-area and power consumption will be compromised. The model and physical implementation of a multi-port PUF (MPUF) was first presented in [17], which is based on the process variations of register file. Later, a reconfigurable multi-port PUF (RMPUF) was proposed in [18], which was designed based on asynchronous clock and fabricated in TSMC 65 nm CMOS process. But energy efficiency was neglected and the power consumptions are still high in [17,18].

To solve the above problems, in this paper we propose a novel class of multi-port and low-power PUF based on MOSFET current-division deviation. Prominent features of the proposed PUF are as follows. Firstly, the proposed PUF is organized in a parallel multi-port scheme that enables the extraction of several bits on each clock cycle, and each output bit is generated by comparing the differential current of the selected current-division cell. Secondly, as a main energy consumption module, the MOSFET current-division array is operated at the subthreshold region which can lead to reduction of power consumption. Thirdly, the proposed PUF is robust to environmental variations, i.e.,

* Corresponding author.
E-mail address: wangpengjun@nbu.edu.cn (P. Wang).

http://dx.doi.org/10.1016/j.mejo.2017.07.017
Received 9 December 2016; Received in revised form 18 June 2017; Accepted 31 July 2017
0026-2692/ © 2017 Elsevier Ltd. All rights reserved.

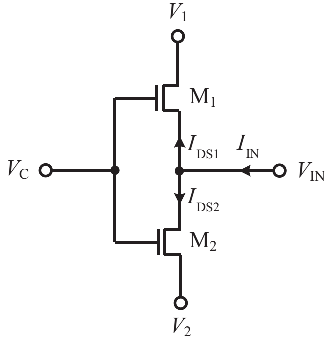

Fig. 1. The MOSFET current-division unit.

the minimum reliability is 98.62% within the 10% fluctuations in supply voltage and – 40 °C to 120 °C temperature range. Finally, it should be noted that all the simulation results are obtained by using the extracted netlist of the designed layout on TSMC 65 nm CMOS process.

The rest of this paper is organized as follows. A brief review of the MOSFET current-division technique and the deviation analysis are introduced in Section 2. The proposed PUF and its elements are illustrated in Section 3. Simulated performances and comparisons are demonstrated in Section 4. Finally, conclusions are drawn in Section 5.

2. MOSFET current-division

2.1. MOSFET current-division technique

MOSFET current-division technique is determined by the symmetry of MOSFET. Although MOSFET exhibits a nonlinear relationship between current and voltage (even in the linear region), the current-division function is linear in nature [19]. Fig. 1 depicts the core of the MOSFET current-division unit, where the common terminal of M_1 and M_2 serves as the current input (the input node voltage is V_{IN}) and other two terminals of M_1 and M_2 serve as the current outputs (the output node voltages are V_1 and V_2, respectively). M_1 and M_2 have the same gate voltage V_C with respect to the substrate. When current I_{IN} is applied to the input node, it would naturally be divided into two parts (I_{DS1} and I_{DS2}), as long as the transistors are in the on-state. The ratio of I_{DS1} to I_{DS2} is given by

$$\frac{I_{DS1}}{I_{DS2}} = \frac{W_1/L_1}{W_2/L_2} \tag{1}$$

where W_1/L_1 and W_2/L_2 are the width to length ratio of M_1 and M_2, respectively. This ratio is independent of the voltages V_1, V_2 and V_C, and is also independent of the operation region of M_1 and M_2. The voltages V_1 and V_2 in Fig. 1 can be set equal to prevent a DC current from flowing through M_1 and M_2.

2.2. Deviation analysis

The *I-V* characteristic of a MOSFET that operates in the sub-threshold region can be approximated by [20].

$$I_{DS} = kV_T^2 exp\left(\frac{V_{GS} - V_{TH}}{mV_T}\right)\left[1 - exp\left(-\frac{V_{DS}}{V_T}\right)\right] \tag{2}$$

where I_{DS}, V_{GS} and V_{TH} are the drain-source current, the gate-source voltage and the threshold voltage, respectively; k, V_{DS} and V_T are the MOSFET gain factor, the drain-source voltage and the thermal voltage, respectively. If V_{DS} is sufficiently larger than V_T (e.g., $V_{DS} > 0.1$ V), the second exponential term of Eq. (2) can be eliminated, and the expression is given by

$$I_{DS} = kV_T^2 exp\left(\frac{V_{GS} - V_{TH}}{mV_T}\right) \tag{3}$$

For the MOSFET current-division unit (shown in Fig. 1) operating at the sub-threshold region, both the gain factor k and the threshold voltage V_{TH} are not the same on account of the process variation. As a result, the I_{DS1} and I_{DS2} will produce random deviations. As the k is uncorrelated with the V_{TH}, the impact of k and V_{TH} on the unit current deviation is illustrated as follows. Firstly, we discuss the case that the threshold voltages of M_1 and M_2 are identical ($V_{TH1} = V_{TH2}$), but random deviation exists in the gain factor ($k_1 \neq k_2$). Thus the current deviation can be expressed as

$$\varepsilon|_{\Delta k} = \frac{I_{DS2} - I_{DS1}}{(I_{DS2} + I_{DS1})/2} = 2\cdot\frac{(k_2 - k_1)V_T^2 exp\left(\frac{V_{GS} - V_{TH}}{mV_T}\right)}{(k_2 + k_1)V_T^2 exp\left(\frac{V_{GS} - V_{TH}}{mV_T}\right)} = \frac{\Delta k}{k_{avg}} \tag{4}$$

where $\Delta k = k_2 - k_1$ and $k_{avg} = (k_2 + k_1)/2$ are the gain factor deviation and the average gain factor of M_1 and M_2, respectively. Secondly, we discuss the case that the gain factors of M_1 and M_2 are identical ($k_1 = k_2$), but random deviation exists in the threshold voltage ($V_{TH1} \neq V_{TH2}$). Thus the current deviation can be expressed as

$$\varepsilon|_{\Delta V_{TH}} = \frac{I_{DS2} - I_{DS1}}{(I_{DS2} + I_{DS1})/2} = 2\cdot\frac{kV_T^2 exp\left(\frac{V_{GS} - V_{TH2}}{mV_T}\right) - kV_T^2 exp\left(\frac{V_{GS} - V_{TH1}}{mV_T}\right)}{kV_T^2 exp\left(\frac{V_{GS} - V_{TH2}}{mV_T}\right) + kV_T^2 exp\left(\frac{V_{GS} - V_{TH1}}{mV_T}\right)} = 2\cdot\frac{1 - exp\left(\frac{\Delta V_{TH}}{mV_T}\right)}{1 + exp\left(\frac{\Delta V_{TH}}{mV_T}\right)} \tag{5}$$

where $\Delta V_{TH} = V_{TH2} - V_{TH1}$ represents the threshold voltage deviation of M_1 and M_2. Finally, the overall current deviations can be described as follows

$$\varepsilon = \varepsilon|_{\Delta k} + \varepsilon|_{\Delta V_{TH}} = \frac{\Delta k}{k_{avg}} + 2\cdot\frac{1 - exp\left(\frac{\Delta V_{TH}}{mV_T}\right)}{1 + exp\left(\frac{\Delta V_{TH}}{mV_T}\right)} \tag{6}$$

In addition, according to the MOSFET mismatching model, the process variation of physical characteristic parameters are inversely proportional to $\sqrt{WL}$. That is to say, the smaller size of MOSFET, the more sensitive of I_{DS} to process variation. Thus, MOSFET with minimum size should be employed to design the deviation generating circuit which is used to capture process variation.

To evaluate the current deviation range and the power dissipation of the MOSFET current-division unit under different control voltage (V_C), we perform 1000 Monte Carlo simulations (three times the standard deviation) for each different control voltage. The simulation parameters are as follows: $V_{IN} = 0.5$ V, $V_1 = V_2 = 0.3$ V, and M_1 and M_2 ($V_{TH} = 0.58$ V) use the minimum size of TSMC 65 nm CMOS process ($W_1 = W_2 = 120$ nm, $L_1 = L_2 = 60$ nm). Then, the mean value of random deviations between I_{DS1} and I_{DS2}, and the average power dissipation and the coefficient variation CV of I_{DS1} (I_{DS2}) are calculated ($CV = \sigma/\mu$, σ and μ represent the standard deviation and the mean value of I_{DS1} (I_{DS2}), respectively). Finally, the statistical results are shown in Fig. 2. As we can see that the MOSFET current-division unit operating at sub-threshold region has the largest deviation range and it also consumes the least power when compared to the unit operating at the saturation region and the linear region.

3. Proposed PUF

3.1. Architecture of the proposed PUF

Fig. 3 shows the overall architecture of the MOSFET current-division deviation based PUF. It is composed of five circuit components, including MOSFET current-division array, decoder, column-selection,

Download English Version:

https://daneshyari.com/en/article/4971159

Download Persian Version:

https://daneshyari.com/article/4971159

Daneshyari.com